

CLAIMS

What is claimed is:

5 1. A processor with secure cryptographic capabilities,
comprising:

 a digital secret that comprises a secret key used in a
key-based cryptographic process, wherein said digital secret
is internally accessible only within said processor;

10 a cryptography engine for performing said key-based
cryptographic process internally within said processor, said
cryptography engine coupled to said digital secret;

 internal memory coupled to said cryptography engine for
supporting said key-based cryptographic process, said
15 internal memory coupled to said cryptography engine.

 2. The processor of Claim 1 further comprising an
internal bus for facilitating secure communication between
said cryptography engine, said digital secret, and said
20 internal memory within said processor.

 3. The processor of Claim 1, wherein said digital
secret is securely confined within said processor.

25 4. The processor of Claim 1, wherein said internal
memory comprises:

microcode for implementing said key-based cryptographic process on data within said processor.

5 5. The processor of Claim 1, wherein said internal memory securely stores intermediate data created within said key-based cryptographic process.

6. The processor of Claim 1, further comprising:
a cryptography unit comprising a functional unit within
10 said processor for securely executing said key-based cryptographic process internally within said processor,
wherein said cryptography unit comprises:

 said digital secret;
 said cryptography engine; and
15 said internal memory.

7. The processor of Claim 1, wherein said key-based cryptographic process comprises:
a key-based encryption process; and
20 a key-based decryption process.

8. The processor of Claim 1, wherein said processor comprises:
a secure hardware environment providing core processing
25 functionality; and
a secure software environment coupled to said secure hardware environment, said secure software environment

generating executable instructions that are sent to said
secure hardware environment for processing, said secure
hardware environment in combination with said secure software
environment providing processor capability, and wherein said
5 secure hardware environment is accessible only through said
secure software environment.

9. The processor of Claim 1, wherein said digital
secret is unique to said processor and is permanently and
10 physically manifested within said processor.

10. A processor with cryptographic capabilities,
comprising:

a secure cryptography unit, wherein said cryptography
15 unit internally provides secure cryptographic capabilities as
a functional unit within said processor, said cryptography
unit comprising:

a cryptography engine for performing a key-based
cryptographic process;

20 a digital secret coupled to said cryptography
engine and accessible only by said cryptography engine,
wherein said digital secret comprises a secret key used
in said key-based cryptographic process; and

internal memory coupled to said cryptography engine
25 for supporting said key-based cryptographic process.

11. The processor of Claim 10, wherein said key-based cryptographic process comprises:

- a key-based encryption process; and
- a key-based decryption process.

5

12. The processor of Claim 10, wherein said processor comprises a very long instruction word (VLIW) processor.

13. The processor of Claim 10, wherein said processor
10 comprises:

a secure hardware environment providing core processing functionality; and

a secure software environment coupled to said secure hardware environment, said secure software environment
15 generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment accessible only through said
20 secure software environment.

25

14. The processor of Claim 10, wherein said digital secret is unique to said processor and is permanently and physically manifested within said processor.

15. The processor of Claim 10, wherein said digital secret comprises:

a plurality of fusible links to manifest said digital secret by permanently setting a binary state in each of said plurality of fusible links.

5 16. The processor of Claim 10, wherein said digital secret comprises a random number that is generated from an HMAC algorithm implemented on testing data associated with fabrication of said IC chip.

10 17. The processor of Claim 16, wherein said testing data comprises:
 wafer test data; and
 die test data.

15 18. The processor of Claim 10, wherein said secure cryptography unit comprises a fully integrated circuit within said processor.

20 19. The processor Claim 10, wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without requiring a bus and which is not susceptible to malicious attack.

25 20. The processor of Claim 10, wherein said key-based cryptography process comprises a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptography process.

21. A processor with secure cryptographic capabilities, wherein said processor comprises:

5 a secure hardware environment providing core processing functionality, wherein said secure hardware environment comprises:

10 a secure cryptography unit, wherein said cryptography unit internally provides secure cryptographic capabilities as a functional unit within said secure hardware environment.

22. The processor of Claim 21, further comprising:

15 a secure software environment for accessing said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability.

20 23. The processor of Claim 21, wherein said secure cryptography unit comprises:

a cryptography engine for performing a key-based cryptographic process;

25 a digital secret coupled to said cryptography engine and accessible only by said cryptography engine, wherein said digital secret comprises a secret key used in said key-based cryptographic process; and

internal memory coupled to said cryptography engine for supporting said key-based cryptographic process.

24. The processor of Claim 23, wherein said internal
5 memory securely stores intermediate data created within said key-based cryptographic process.

25. The processor of Claim 21, wherein said secure
cryptography unit comprises a fully integrated circuit within
10 said processor.

26. The processor of Claim 23, wherein said secure
cryptography unit comprises a fully integrated circuit within
said processor to facilitate communication between said
15 cryptography engine, said digital secret and said internal memory without requiring a bus.